Executive Summary

During the February 2009 AUSA Winter Conference, the Army will announce publication of FM 3-36, ***Electronic Warfare in Operations***. This is the first new Electronic Warfare (EW) doctrine in more than a decade. Production and publication of such new doctrine was needed because old doctrine had faded into irrelevance following the close of the Cold War, having not been updated to reflect new full spectrum requirements, current organizational structures, or needed adjustments to meet emerging joint requirements. With the publication of FM 3-36, the Army reaches a key milestone in rebuilding a vitally needed EW capability that it had allowed to atrophy. The new FM describes the application of EW in support of full spectrum operations and will serve as a baseline for ensuring a common understanding and consistency for training as well as for developing operational plans, orders, standard operating procedures, and directives.

In addition, it should be also noted that publication of this new EW doctrine comes close on the heels of an announcement by the Army made 26 January 2009 regarding the establishment of new EW career fields (Functional Area/Military Occupational Specialty 29) for officers, warrant officers, and enlisted personnel. Over the next three years, approximately 1,700 EW personnel will be added to units from company to Army Land Component Command levels, who will provide, among other responsibilities, direct support for effectively managing and deconflicting use of the electromagnetic spectrum (EMS) at every level of command, jamming enemy use of the EMS, and countering such threats as those posed by Radio Controlled Improvised Explosive Devices (RCIEDs). Another approximately 2,100 additional EW personnel are planned to be added in the out years. These signal achievements have been reached as part of a broad range of initiatives still underway across the DOTMLPF spectrum to ensure that the Army's emerging EW force is proficiently trained and properly equipped to perform their missions.

Irrespective of the good news reflected in the reaching of these two recent milestones, it would be well to bear in mind that EW is a legacy capability which is being rebuilt and refurbished, not initially introduced into the Army. The recently rediscovered recognition of EW's importance within the Army does not constitute the introduction of cutting edge capabilities that will be needed in the future to deal with emerging threats posed by new and startling technological developments occurring both now and in the future. The Army's experience and a growing understanding of the complex networked world are already creating a need to move out of the past and into a new cyber-electronic environment.

As a result, as we consider the grave challenges with which the Army must prepare to deal in the future, we must move beyond EW to acknowledge and prepare vigorously for dealing with adversaries who are seeking emerging "game-changing" technologies to be employed as part of the various brands of hybrid or unrestricted warfare many experts are predicting as the norm of the global security environment. Among such threats of greatest concern are those presented by the integrated and combined use of cyber networks and EMS technology to attack computer networks and communications systems of both governments and their military forces in a systematic way.

Complicating the future security environment is the burgeoning of publicly available commercial technology in both cyber space as well as use of the EMS. Easy public access to such technologies creates additional challenges as adversaries find new opportunities for exploiting cyberspace, space, and the broader Electromagnetic Spectrum (EMS) for nefarious ends that are difficult to prevent. This is reflected in the proliferation of use by acknowledged terrorists of both webpage technology as well as communications devices of the "wireless world" where networks are merging and handheld computing devices are exponentially increasing in capability. Moreover, it is useful to note that both state sponsored as well and non-state adversaries are able to access these technologies and adapt them to their needs.

Irrespective, we at CAC see in such advances not only potential threats, but great opportunities. As such, the Combined Arms Center has recently embarked on a series of initiatives with regard to exploring how best to develop and integrate such emerging cyber technologies both across the Army as well as nested within the broader Joint Community. To this end, CAC is sponsoring an Information and Cyberspace Integrated Capabilities Development Team (I&C ICDT), which was established in September 2008, to fully research, analyze, and make recommendations on Army required information, cyberspace, and C-E capabilities. One immediate consequence has been that doctrine is already under revision in response to military operations that are occurring in an increasingly complex operating environment. We intend to follow a similar DOTMLPF process as was used for rebuilding of EW within the Army to ensure that the Army develops the required cyber capabilities to provide effective countermeasures as well as offensive options to future commanders having to deal with such threats in the operational environment of the future.